

# The scenario of Nomadism

## 1. Background

User security here and now: its fragility, its dependence and the “big brother syndrome” in locating individuals.

Nomadism (intermittent connection and activity from various locations) or mobility (continuous connection to a digital infrastructure and activity during the move) destabilize the perennial framework within which personal cyber-sphere security was organised while the position was static. The security of mobility requires an anchor of geography and time. Nomadism and mobility especially emphasize the logic of a spatiotemporal security framework based on the “here and now” (*hic et nunc*).

The “here” is defined as a provisional location, simply designated by our movement, either voluntarily and consciously by us (it is, thus, an authentication with time and space for comfort, an alibi or a deliberately accepted condition), or in spite of us, via location tracking.

The designation and knowledge of “here” faces several decisions about who is implementing the action, with the agreement of whom, towards whom and by what technical means.

The concept of geographical territory, where legislation applies, retains its relevance in the sense that it remains necessary, for the common safety, to report both the actual act committed by an identifiable author, as well as the point of entry from where the actions have been initiated originally.

The “now” introduces and facilitates an *in vivo*<sup>1</sup> environment, which corresponds to the ICT specificities: capacity for near-instantaneous, customisable, interaction or adaptation to a person.

In order to protect this volatile mobile digital life, made in real time and *in vivo*, several alignments are possible:

- Protect our secrets and our identities in terms of identification and authentication, with tools and components such as secure USB keys, smart cards, SIM cards, etc. This would secure on the one hand, the individual, and on the second, the digital instruments of the individual. This would be very useful for those who are engaged in online videogames, with multiple players or multiple parties.
- Develop a contextual security (ambient intelligence), to deal with problems such as:
  - Tracking, monitoring and traceability of people, according to their trajectories or refined observations of their behaviour (e.g. through a crosschecking between input position and images of networks of urban cameras). This monitoring may be as much a source of protection – to validate remote access by an individual by seeking identity, for example – as a source of privacy violation.
  - Usability of security tools; awareness of the user’s security; defining a fair balance between making an activity dependent on the awareness of its user, with the capacity for him to easily disengage or configure these functions at

---

<sup>1</sup> Real-life, uncontrolled; literally - “within the living”

will. An acceptable level of usability requires mediation with both technical and citizen needs.

- Contingency plans required for the consequences arising from the extension of itself that is the computer science tool; when this tool breakdowns, malfunctions or maliciously taking control. There is a risk, in regard to a dependence on both the physical and psychological integrity of an individual to keep this tool committed to memory: its links with the past, with the outside world, and particularly in need of communication, in crisis situation, etc.
- Provide tools and means to ensure privacy around personal objects: this affects, in particular, the “Internet of Things”, and the capacity to delegate security to external entities: robot, micro-robots (medicine, digital prosthesis) or other artefacts. This issue raises the question of delegation (to whom, for what) for objects in our daily lives such as our car, in a multiparty situation (vehicle owner, repairman, car manufacturer).

For these objectives, it seems reasonable to defer to a type of trust infrastructure, rather than a security infrastructure.

## **2. Vision**

Personal (hardware, software, data) cyber-sphere security: the digital objects’  
life-cycle security

The scenario of Nomadism reinforces the need to achieve a mastery of the life-cycle of information and its secure media. An individual becomes, through the information society, a constant producer of this raw material: information on him, his past, his journey, etc. Being a creator of information does not, however, automatically give someone control of their personal cyber-sphere.

This evolution requires a check by each creator on their data, at anytime during the life-cycle of his information. One way could be a personal dedicated overlay network, of which each person would have control. A potential solution would be to also provide tools (such as garbage collection in computer memory for object oriented language) that could go and destroy (or in the computer memory analogy, “put in the trash”) the information that is private but which is exposed to any third party. In a life-cycle perspective, it would therefore be a tool that ensures the final phase of the information cycle is “cleaned” by a garbage collector, which is activated at will.

## **3. Roadmap**

Redistribution of responsibility in the chain of actors involved in exchanges

In a situation of mobility, it is necessary to facilitate and clarify the roles between the various ICT actors, in order to better identify the responsibilities and duties of each player (telecommunications operators, network operators, service providers, content or service providers, etc.). The issue of maintaining a mutual or collective security system should be strengthened, as the number of these players tends to grow.

One possible way should be through security at the virtualization level: virtualization of all the paradigms (packets, routers, channels, bandwidth, sessions, applications, etc.).

A second key point relates to the necessary rebalancing of the relationship between supplier and user, including the individual user. This unequal and unfair face-to-face relationship is today marked by a strong asymmetry: the provider has legal power, which causes a significant imbalance. A shift in this balance, resulting in the enhanced usage, access and control of the user over their digital sphere will ensure the enhanced development of services, including their commercial viability

It is important to achieve sustainable forms of governance in the user's info-sphere: structures capable of supporting growth in mass service deployment, on a scale of hundreds of millions of users. This comprises both the management of data and its traces and trails left on the network. This pertains to any solution based on the ability to audit what is happening on a network – to identify trends and points of entry – while maintaining sufficient digital privacy for everyone.

It is questionable, however, as to whether the *in vivo* might not lead to a creeping form of *in vitro*<sup>2</sup>, in the sense that the digital space of a person may give rise to enclosed domain of freedom, in the form of monitoring and observation of actions, gestures and movements, and maybe even their opinions.

---

<sup>2</sup> Controlled environment; literally - "Within the glass"